

# Market Guide for Information-Centric Endpoint and Mobile Protection

**Published:** 26 October 2016    **ID:** G00313266

**Analyst(s):** John Girard

## Summary

In a world that emphasizes connectivity, mobility, sharing and cloud services, business information flows continuously in and out of endpoint devices. Security and risk management leaders must develop a portfolio of solutions to address different aspects of encryption and boundary defense.

## Overview

### Key Findings

The fact that data breaches involving endpoints continue to be reported at alarming rates clearly indicates that conventional approaches are not sufficient to protect business information in an increasingly interconnected and mobile world.

Companies seeking business information protection tend to purchase point solutions that do not holistically address the realities and risks of data movement.

Gartner has identified nine different methods for information-centric endpoint protection. Vendors are expanding their capabilities to more completely address the different methods and reduce leakage risks.

### Recommendations

Security and risk management leaders focused on endpoint and mobile security must:

Use Gartner's market analysis to understand and identify the differences between different methods of protection, and the potential gaps between those methods in your organization.

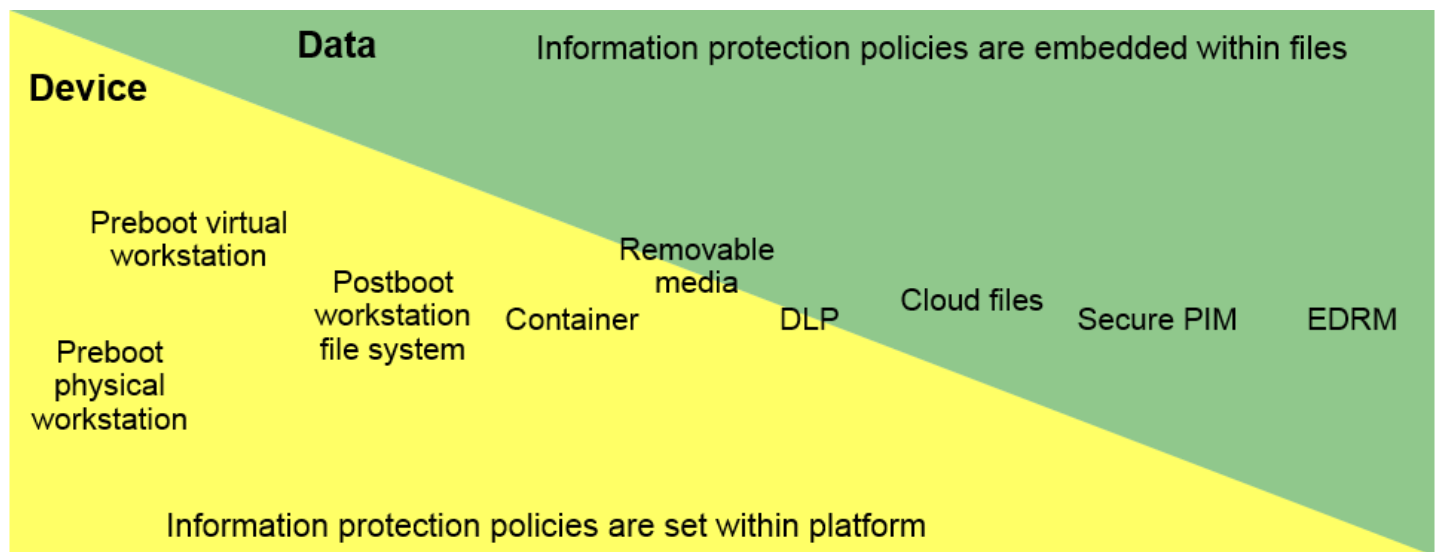
Choose products to build a blended defense to minimize unplanned and unauthorized movement of business information across all business endpoints.

Choose vendors that invest in standards for information protection interoperability, performance and portability across protection methods.

## Market Definition

Endpoint systems are porous, and users can be careless. Information-centric security is the last line of defense of data when firewalls, anti-malware tools, best practices and other traditional defenses fail. Products included in this market guide vary in their methods, but all pursue the same fundamental protection goal: to block file access from unauthorized people or circumstances, and they can do this by means of up to nine different methods, as illustrated in Figure 1.

**Figure 1.** Comparing the Scope of Information-Centric Endpoint Protection Methods



Source: Gartner (October 2016)

These nine protection methods range from coarse approaches, protecting an entire disk drive, to granular ones, extending policies to individual files, through rights management. In a world where information can move constantly and systems are continuously connected to the internet, products that qualify for this study encrypt and protect files at points ranging from endpoint preboot to application, for on-device storage and for files moved to external destinations. Policies for access controls are managed centrally and can be pushed to individual endpoint systems. Rules can be set to expire access to devices, file systems and files. Endpoint devices report their statuses to verify compliance. Products in this report are software-based, and rely on endpoint device agents to maintain policies and protections. Vendors are expected to run on popular endpoint platforms, and to support industry standards for encryption, such as U.S. Federal Information Processing Standard (FIPS) 140-2 and other international certifications as appropriate, including Common Criteria (CC). All suitable embedded cryptography (crypto) and accelerator techniques should be used. The list includes native crypto for Windows (BitLocker), Mac OS (FileVault 2), inbuilt crypto engines for iOS and Android devices, Trusted Platform Modules (TPMs) for key storage, AES New Instructions (AES NI) for Intel CPU crypto acceleration, and self-encrypting drives (SEDs) for maximum disk response.

## Market Direction

While there is not a single method to solve all aspects of information protection, there is a single problem with a single desired outcome: Data losses are at an all-time high,<sup>1</sup> and data breaches — both criminal actions and careless accidents — must be prevented by any and all means.

The competitive opportunity for vendors in this Market Guide is to broaden common policy frameworks and close up points of vulnerability by adopting more of the nine protection methods charted in Table 1. A major success factor involves the reconciliation of keys and key management applied to different layers of encryption. Security and risk management leaders will find few comprehensive solution providers today, and should monitor the progress of vendors that show evidence of building more inclusive information-centric solutions. Consolidation means fewer layers of encryption and keys, leading to easier administration and improved scalability.

This report is the successor to the "Magic Quadrant for Mobile Data Protection Solutions," last published in 2015. The previous definition of mobile data protection was centered on full-disk encryption (FDE). In 2016, all information is potentially mobile; disk encryption is only a piece of the solution; and protection solutions must account for the many ways that business information needs protection as it moves.

## Market Analysis

Information defense technologies have been developed as point solutions to solve narrow parts of the data leakage problem for buyers with limited expectations. The interconnected world and its increasingly pervasive data-sharing demands will soon force companies to put the solutions together to resolve different aspects of leakage. Full-disk and file system encryption will always play the first line of defense. Enforced protection for peripheral file transfers, such as

flash drives, maintains encryption control over local ports. Containers and "secure PIMs" provide methods to quarantine specific parts of business information workflow for particular usage patterns. Data loss prevention (DLP) and cloud file protections will trap and protect data movement to and from network resources. And enterprise digital rights management (EDRM) can imbue files with persistent encryption in coordination with rights-aware apps. Each of these methods is a piece of the information protection solution. Used together, these methods overlap each other's weaknesses to reduce the risks of data leakage (Table 1).

**Table 1.** Defining Information-Centric Endpoint Protection Methods

Method	Protection Analysis	Failure Scenarios
Preboot encryption of physical workstation	<p>The primary system disk is encrypted and protected by a preboot agent (PBA). The OS cannot boot without successful user login to the PBA. This method is optimized for single users on single workstations. Boot behavior can be modified if a device is powered up on a trusted network.</p> <p>Defense value: The OS and user data on the primary disk of a powered-down or locked device are completely unreadable.</p>	If the system disk is unlocked after boot, then it is vulnerable to typical attack vectors. Some companies bypass the preboot agent to shorten boot time, and lose full protection as a result.
Preboot encryption of virtual workstation	<p>The primary system image is virtual. The system image is unreadable without successful user login. This method is optimized for single users on single virtual images.</p> <p>The primary system virtual image is encrypted and protected by a PBA. The OS in the virtual image cannot boot without successful user login to the PBA. This method is optimized for single users on single workstations. Boot behavior can be modified if an image is powered up on a trusted network.</p> <p>Defense value: The OS and user data on the primary virtual disk of a powered-down or locked image are completely unreadable.</p>	If the virtual system disk is unlocked after boot, then it is vulnerable to typical attack vectors. Virtual images may not fully take advantage of hardware and OS security features.
Postboot workstation OS file system encryption	<p>This is an alternative to full-disk encryption. This method is suitable for multiple users on shared workstations. Selective reasons to encrypt may be applied, such as folder location or file type, but this is not a DLP or EDRM solution.</p> <p>Defense value: The OS can start, but selected user files and configurations are unreadable without user login. Automated OS patch and update, as well as disk maintenance, are easier to perform, even in an unattended situation such as wake-on-LAN.</p>	If user data can be unlocked after boot, then it is vulnerable to typical attack vectors. Protection is not guaranteed to be persistent. Selective access controls for different types of files can impact usability.

Method	Protection Analysis	Failure Scenarios
Container	<p>Files are unreadable without successful login to protected partition/container. App access to container and import/export of files may be controlled. Some containers may include DLP features. This method is suitable for shared systems and multiple users.</p> <p>Defense value: Information protection is independent of OS and disk protection, and can be highly portable. Containers can be context-dedicated to specific business processes or act as a broad workspace.</p>	User data access is determined by policy and requires that apps are configured to work in quarantined file spaces. In some cases, protection policies might be relaxed in response to usability complaints.
Removable media encryption	<p>Files can be forced into encryption by the OS at the moment of copying to external media, such as flash drives or DVDs. Most products can keep a log of files written to flash drives. DLP-style policies can be added for specific reasons to encrypt. This method is suitable for shared removable media.</p> <p>Defense value: Information protection is independent of OS and disk protection, and can be highly portable.</p>	The process is imperfect, as some file transfers could be missed. Once unlocked, files are difficult to impossible to track in subsequent use. Flash drives are difficult to track or remotely wipe. Other external media types may not be treated consistently. For example, a tethered phone with addressable storage may not be treated like an external flash drive.
DLP controls	<p>File transfers can be blocked or processed with encryption based on keywords, user, project and other contexts. This method is suited to context-dependent data protection.</p> <p>Defense value: Data transfer events can be identified and evaluated using business rules and policies.</p>	The recognition process is imperfect and made complex by the need to predefine categories of acceptable and unacceptable transfer events. In some cases, protection policies might be relaxed in response to usability complaints.
Cloud file encryption	<p>File transfers are processed with encryption for EFSS. This may be a specific application of DLP and DRM — data readability can be limited to user groups, project IDs and so on. Key control over encrypted data can be held by the company rather than by the EFSS provider.</p> <p>Defense value: Data transfer events can be identified and evaluated using business rules and policies.</p>	The recognition process is imperfect due to the many variations of cloud sharing and backup services. Key management can be complex when scaled. In some cases, protection policies might be relaxed in response to usability complaints.

Method	Protection Analysis	Failure Scenarios
Secure PIM	<p>Email and calendar are quarantined to a dedicated, contained PIM app that prevents forwarding to unknown destinations and maintains self-encryption of all PIM data.</p> <p>Defense value: Email and calendar are among the highest demands for external business information access. Secure PIM may be an effective single-purpose drop-in solution for users on unmanaged devices.</p>	Secure PIM is generally unpopular for users. In some cases, protection policies affecting email forwarding and attachment handling might be relaxed in response to usability complaints.
EDRM	<p>This method is suited to context-dependent data protection. Files are imbued with persistent protection policies when created, read and updated. The policies can specify access by company, user, project, and other details. EDRM can also stipulate limitations on app behavior such as blocking "save as," clipboard copying, printing and so on.</p> <p>Defense value: EDRM creates the tightest possible access control relationships between files and apps. Policies can be detailed, and access can be tracked.</p>	EDRM is difficult to scale and to apply horizontally, meaning its use can be curtailed even when otherwise mandated. A lack of standards creates interoperability problems. Rights policies with expiration dates might be tricked by backdating system calendars.

Source: Gartner (October 2016)

## Representative Vendors

*The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.*

Eighteen vendors are chosen as representative in this guide. There are 12 vendors from the 2015 "Magic Quadrant for Mobile Data Protection Solutions" (a 13th is out of business) and another six that offer workstation containers, DLP and EDRM. These vendors are frequently mentioned in endpoint information protection inquiries, and they primarily target workstation platforms, meaning PCs running Windows and Mac OS X. Support for nonworkstation platforms is noted, but the vendor list is not automatically extended to enterprise mobility management (EMM) vendors, which are mainly focused on iOS and Android. Table 2, which follows the vendor write-ups, compares vendor capabilities based on the nine methods set forth in the Market Definition section. A check mark does not mean that the vendor offers a capability on all of its supported platforms. This is not an exhaustive list, and other vendors may meet business needs as well or better.

### Accellion

accellion.com (<http://accellion.com/>)

Accellion, a California-based company, provides a secure enterprise file synchronization and sharing (EFSS) solution called kiteworks. Accellion kiteworks embeds rights-managed encryption into outbound files and can set limits on access, including authentication challenges and expiration dates. The kiteworks solution can be deployed as a private cloud on-premises (virtual appliance on-premises), as a private hosted cloud (via Amazon Web Services [AWS] and Microsoft Azure) or as a hybrid cloud. Accellion kiteworks integrates with a wide range of third-party repositories, including Box, Dropbox, Google Drive, Microsoft OneDrive, Microsoft Exchange, Microsoft SharePoint, and others.

Accellion also offers the Accellion Secure Mobile Productivity suite, which allows customers to create and edit Office files (Word, Excel and PowerPoint) on mobile devices. Windows, Mac OS X, iOS, Android and Windows phone. Certifications include FIPS 140-2 and security operations center (SOC) 2 Level 1, with FedRAMP in process.

## **BlackBerry**

[www.blackberry.com](http://global.blackberry.com/en/home.html) (<http://global.blackberry.com/en/home.html>)

BlackBerry, based in Canada, provides a mobility software suite with capabilities that cover many areas of information-centric endpoint protection. These capabilities include persistent information rights management for file and media sharing (via acquisition of WatchDox), isolation and DLP of critical enterprise data via application security containers (via acquisition of Good Technology), full device encryption in BlackBerry's mobility solutions suites for Android and BB10, FIPS 140-2 certified cryptographic software, key management (via acquisition of Certicom), secure PIM, and so on. The BlackBerry Enterprise Mobility Management solution supports iOS, Mac OS, Android, BB10 and Windows 10. The company holds Common Criteria EAL 4+ certifications for the isolation/DLP technology and PIM suite.

## **Bufferzone**

[bufferzonesecurity.com](http://bufferzonesecurity.com/) (<http://bufferzonesecurity.com/>)

Bufferzone is an Israel-based company that has developed a strict virtual container to protect company applications, including web browsers, email, Skype, FTP and even removable storage. Bufferzone is transparent to both the application and the end user, yet completely seals off threats from the rest of the computer. Bufferzone isolates malware and prevents it from doing harm by confining it at the boundary of the container, and supports DLP controls for files leaving the container. Bufferzone runs on Windows.

## **CenterTools Software**

<https://www.drivelock.de> (<https://www.drivelock.de/>)

CenterTools Software, based in Germany, has offered DriveLock since 2003. In addition to FDE, DriveLock File Protection offers transparent file-based encryption on removable drives, network shares and local disks. DriveLock can be configured to encrypt individual local files and folders independently of full-disk encryption. Also supported are containers consisting of encrypted virtual file systems, which can be created locally and then shared. In fact, both transparent encryption modules (file-and-folder and full-disk) are entirely independent of each other (they can be used separately or combined). DriveLock offers access controls and transparent file-based encryption of files in common cloud-based sync clients such as Dropbox, Google Drive and OneDrive. Platform support is provided for Windows 7 through 10, Mac OS X iOS, Android and Linux. CenterTools owns the Gemalto (SafeNet) cryptographic module for FDE, which is FIPS 140-2 certified to Level 2 in software, and uses FIPS-certified OpenSSL for file and folder encryption. Additional support is provided for Intel AES NI and UEFI.

## **Check Point Software Technologies**

<https://www.checkpoint.com> (<https://www.checkpoint.com/>)

Israel-based Check Point Software Technologies has offered FDE and removable media encryption since 2007, using technology acquired from Pointsec, which had been a player in the mobile data protection market since the 1990s. The FDE is OS-independent, using Check Point's crypto engine. Check Point's DLP software blade offers wide coverage of traffic transport types, including protection for data in motion, as well as transparent, content-aware document security protection of mail attachments, web files and FTP. Users may encrypt data on the document level for authorized users only, and optionally set an expiration date. This encryption can be applied automatically based on DLP data type classification, file location and file properties. Platform support is provided for Windows and Mac OS X. Check Point is FIPS 140-2-certified to Level 1, and was awarded CC EAL4. Additional support is provided for UEFI, Opal SEDs and Trusted Platform Modules.

## **Dell**

[www.dell.com/datasecurity](http://www.dell.com/datasecurity) (<http://www.dell.com/datasecurity>)

Texas-based Dell offers a la carte solutions as well as the Dell Data Protection | Endpoint Security Suite Enterprise, built on technologies acquired from Credant Technologies in 2012. Dell provides a data-centric, policy-based approach to full-disk, file and removable media encryption for a wide variety of physical, mobile and persistent virtual platforms. Supported platforms include Windows XP, 7, 8+, 10+, Windows Server, VMware vSphere and Horizon, Microsoft Hyper-V, Citrix XenDesktop, Mac OS, iOS, and Android devices. Extensions will protect data transferred through popular cloud sync-and-share services (including Box, Dropbox, Google Drive and Microsoft OneDrive) and removable media (such as USB keys and optical drives). Dell's Endpoint Security Suite Enterprise includes encryption, authentication and advanced threat prevention for the endpoint, all managed by a single console. Dell is certified to FIPS 140-2 Level 2 in software. Additional support is provided for BitLocker, FileVault 2, SEDs, TPM (including 2.0), legacy bios (Windows 7) and UEFI (Windows 8/10).

### **Digital Guardian**

<https://digitalguardian.com> (<https://digitalguardian.com/>)

Based in Massachusetts, Digital Guardian, formerly Verdasys, is a longtime content-aware player with premium tools focused on encrypting and protecting intellectual property in a DLP framework. The vendor has a global presence, but does two-thirds of its business in North America. Platform support includes Windows 7 through 10, and Mac OS X and Linux distributions, including Red Hat, CentOS, Oracle, SUSE and Ubuntu. A fully compatible Digital Guardian app is offered for iOS. Digital Guardian core code is certified to FIPS 140-2 Level 1 and was awarded CC EAL2+.

### **EgoSecure**

<https://egosecure.com> (<https://egosecure.com/de/>)

EgoSecure, based in Germany, acquired the FDE solution of Secure, a Swiss software maker, in 2014. This solution is now EgoSecure Full Disk Encryption, which is a part of the larger EgoSecure Data Protection product. EgoSecure integrates user behavior analysis (called Insight) with disk and file encryption solutions. Insight answers security-related planning questions in the form of clear graphs and tables, and thereby provides facts to configure the necessary encryption policies for FDE, removable media, cloud storage, folders, network shares, content filters and granular external device control. Supported platforms include Windows XP, Vista, and 7 through 10, as well as Android and iOS. EgoSecure is certified to FIPS 140-2 Level 1 in software.

### **Fasoo**

[en.fasoo.com](http://en.fasoo.com) (<http://en.fasoo.com/>)

Based in South Korea, Fasoo's Data Security Framework performs discovery, classification and protection by scanning company file systems. Files are automatically classified and encrypted as they are created through desktop or server applications, or extracted from databases. Policy attributes are dynamic and travel persistently with files to control policies such as the right to view, edit, copy, paste, print, capture or decrypt. Fasoo data security products support Windows, Mac OS, iOS and Android platforms, and use FIPS 140-2 certified encryption modules.

### **Kaspersky Lab**

[kaspersky.com](http://kaspersky.com) (<http://kaspersky.com/>)

Kaspersky Lab, headquartered in Russia, has provided a workstation encryption solution since 2013. Platform support is provided for Windows 7 through 10. Kaspersky's endpoint protection suite and removable media protection, as well as its basic EMM for Apple iOS and Google Android and Samsung Knox smartphones and tablets, are integrated in a single offering. Kaspersky has been awarded FIPS 140-2 certification for cryptography. Additional support is provided for AES NI.

### **McAfee**

[www.mcafee.com](http://www.mcafee.com) (<http://www.mcafee.com/us/index.html>)

McAfee, an Intel company based in California, provides full-disk, file-level and removable media encryption and DLP in its Complete Data Protection suites. Platform support is provided for Windows 7 through 10, and for Mac OS X. Support for consumer smartphones and tablets is offered in a separate product, McAfee Enterprise Mobility Management, which

reports into a single integrated console. McAfee is certified to FIPS 140-2 Level 1 in software and was awarded CC EAL4. Additional support is provided for BitLocker, FileVault 2, Intel AES NI, UEFI and Opal SEDs.

## Microsoft

[www.microsoft.com](http://www.microsoft.com/) (<http://www.microsoft.com/>)

Microsoft, based in Washington, provides the embedded BitLocker engine to encrypt hard drives, including those on virtual machines, and external media in certain OS versions. It also offers a central management system, Microsoft BitLocker Administration and Monitoring (MBAM), for companies that are licensed for Microsoft Desktop Optimization Pack (MDOP). Manageable file-level encryption that enables data separation and containment is now offered through Windows Information Protection (WIP), which was added to the Windows 10 Anniversary Update. Microsoft Azure Information Protection provides classification assistance as files are created or modified. Office 365 DLP and message encryption work across Office apps, as well as Exchange email, SharePoint and OneDrive. A component of Intune is needed to fully enforce managed app DLP policies on iOS and Android. Microsoft Rights Management service (RMS) applies persistent policies to files to control use rights, copying, saving and so on. RMS works across Windows, Mac OS X, iOS and Android and can protect all types of files. RMS is validated to FIPS 140-2 Level 2 when combined with hardware security modules. BitLocker and MBAM are certified to FIPS 140-2 Level 1 in software. There is additional PC support for TPM, UEFI and Opal SEDs.

## Seclore

[www.seclore.com](http://www.seclore.com/) (<http://www.seclore.com/>)

California-based Seclore facilitates security in external collaboration. Seclore provides persistent and format/device/sharing-independent security for documents and email. The solution includes standard EDRM features, such as native app access, classification support, support for Windows XP to 10, Mac, iOS and Android, revocation, and information-centric audits. Advanced features are also provided, such as location-based controls for data residency requirements, pluggable encryption, bring your own key (BYOK) and FIPS-140-2-compliant encryption. Files downloaded from any enterprise application can be automatically protected with the source system security policies. Seclore maintains more than 80 connectors for identity and SSO systems, including but not limited to Active Directory (AD), Lightweight Directory Access Protocol (LDAP), Security Assertion Markup Language (SAML), OAuth, enterprise content management (ECM) and EFSS (such as Box, Citrix ShareFile, IBM ECM, Microsoft SharePoint and Dell EMC Documentum), messaging systems (including Microsoft Outlook, IBM Notes, and Gmail), DLP systems (including Symantec and McAfee), transactional and analytics systems (such as SAP and SQL Server Reporting Services [SRSS]), and security information and event management (SIEM) systems (including HPE Security ArcSight, and Splunk). An API is offered to develop additional connectors. Supported platforms include Windows (from XP through 10), Mac OS X, iOS and Android. Encryption is certified to FIPS 140-2, and SAP has certified "Seclore Rights Management for SAP."

## Sophos

[www.sophos.com](http://www.sophos.com) ([../.../Users/aflounde/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.Outlook/ZS5VP7LF/www.sophos.com](http://www.sophos.com))

Sophos, headquartered in Oxford, U.K., offers SafeGuard Encryption, a hard drive and external media encryption product built on technologies originally acquired from Utimaco. Platform support is provided for Windows and Mac OS X, and iOS and Android. Sophos Mobile Control provides additional file encryption, container and secure PIM functionality on iOS and Android. File-based encryption can be set up as an alternative to FDE or to run in parallel. The company's design for "synchronized encryption" adds DLP and persistent DRM protections for files transferred between devices and external destinations, such as USB and EFSS, including policies for read, write, save and so on. Protected files can be placed in HTML5 encryption wrappers at the time of transfer to external storage or email. Sophos is certified to FIPS 140-2 Level 1, and was awarded CC EAL3+ and CC EAL4. Additional support is provided for FileVault 2, BitLocker, TPM, Opal SEDs, Intel AES NI, vPro and UEFI.

## Symantec

[www.symantec.com](http://www.symantec.com) ([../.../Users/aflounde/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.Outlook/ZS5VP7LF/www.symantec.com](http://www.symantec.com))



Symantec's Symantec Endpoint Encryption (SEE) is a hard drive and external media encryption product built upon technologies acquired from PGP and GuardianEdge. Optional components Symantec Desktop Email Encryption and Symantec File Share Encryption add features to block unauthorized file transfers and to protect approved files and folders in transit. Platform support includes Windows 7 through 10, and Mac OS X and Linux distributions, including Ubuntu, RHEL, CentOS, SUSE and SUSE Linux Enterprise Server (SLES). The optional Symantec Mobile Encryption for iOS facilitates the sending and receiving of PGP-encrypted email on iPhones and iPads. Also supported are FileVault 2 and Intel AES NI BitLocker and Opal SEDs. Symantec Encryption products use FIPS 140-2 Level 1-validated cryptography, with plans to continue Common Criteria certification on an ongoing basis.

## Titus

[www.titus.com](http://www.titus.com) (<http://www.titus.com/>)

Titus, a Canadian-based company, provides data discovery and classification as a DLP function to secure sensitive email, documents and other file types on workstations, mobile devices and cloud services. Titus Classification Suite scans and applies metadata to unstructured information, with the option of employing automatic or user-led classification by involving end users in classification as they create email and documents. Titus Illuminate scans and inventories on-premises file shares, Box, Dropbox, Microsoft OneDrive and Microsoft SharePoint, and examines and automatically classifies the files it discovers. Titus Classification for Mobile provides a secure container for business documents, with direct access to corporate SharePoint libraries and common cloud sharing services. Titus interoperates with Microsoft RMS and Ionic Security, and can preserve access rights to encrypted files on workstations. Titus extends Microsoft Rights Management services (RMS) to mobile devices, allowing users to access email and files protected using Microsoft RMS.

## Trend Micro

[www.trendmicro.com](http://www.trendmicro.com) (<http://www.trendmicro.com.sg/sg/index.html>)

Trend Micro, based in Tokyo, Japan, offers an FDE drive and removable media encryption built from technologies acquired from Mobile Armor in 2011. In addition, it offers integrated DLP controls, cloud file encryption and email encryption. These, as well as other endpoint protection platform capabilities, are offered as part of the Smart Protection Suite for Endpoints and are managed under a common console. Platform support is provided for Windows 7 through 10, Mac OS X, iOS and Android. Linux is also supported for email encryption on the gateway. Trend Micro is certified to FIPS 140-2 Level 2 and was awarded CC EAL4+. Additional support is provided for BitLocker, FileVault 2, Seagate and SanDisk, Opal SEDs, TPM, and Intel AES NI.

## WinMagic

[www.winmagic.com](http://www.winmagic.com) ([../../../../Users/aflounde/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.Outlook/ZS5VP7LF/www.winmagic.com](http://../../../../Users/aflounde/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.Outlook/ZS5VP7LF/www.winmagic.com))

WinMagic, headquartered in Canada, has sold complete workstation encryption solutions since 1997. SecureDoc is geared toward companies with high security needs and strong authentication requirements. Platform support is provided for Mac OS X, Windows 7 through 10 and all major Linux distributions, with and without SEDs. Fully managed and compatible SecureDoc agents have also been released for popular smartphones and tablets. Additional support includes TCG Opal and Enterprise SEDs, TPM, Intel AES NI, BitLocker, FileVault 2, and UEFI. WinMagic is certified to FIPS 140-2 Level 1 and was awarded CC EAL4.

**Table 2.** Chart of Vendor Capabilities: Vendors, Products and Information Protection Methods

Vendor and Example Product	Preboot Workstation: Physical	Preboot Workstation: Virtual	Postboot: OS File System	Container	Media	DLP	Cloud	Secure PIM	EDRM
Accellion kiteworks				✓		✓	✓	✓	

Vendor and Example Product	Preboot Workstation: Physical	Preboot Workstation: Virtual	Postboot: OS File System	Container	Media	DLP	Cloud	Secure PIM	EDRM
BlackBerry BlackBerry Enterprise Mobility Management Suite	✓		✓	✓	✓	✓	✓	✓	✓
Bufferzone Endpoint Security Solutions				✓	✓	✓			
CenterTools DriveLock	✓	✓	✓	✓	✓		✓		
Check Point Full Disk Encryption Software	✓	✓		✓	✓	✓			✓
Dell Dell Data Protection   Encryption Enterprise Edition	✓	✓	✓	✓	✓		✓		
Digital Guardian Digital Guardian				✓	✓	✓			
EgoSecure Data Protection	✓	✓	✓		✓	✓	✓		
Fasoo Enterprise DRM, eData Manager, RiskView					✓	✓	✓		✓
McAfee Complete Data Protection	✓	✓	✓		✓	✓	✓		

Vendor and Example Product	Preboot Workstation: Physical	Preboot Workstation: Virtual	Postboot: OS File System	Container	Media	DLP	Cloud	Secure PIM	EDRM
Kaspersky Lab Endpoint Security	✓	✓	✓		✓	✓	✓		
Microsoft BitLocker, Azure Information Protection, RMS	✓	✓	✓	✓	✓	✓	✓	✓	✓
Seclore EDRM							✓		✓
Sophos SafeGuard, Mobile Control	✓	✓	✓	✓	✓	✓	✓	✓	✓
Symantec Endpoint Encryption	✓	✓		✓	✓	✓	✓	✓	
Titus Classification Suite					✓	✓		✓	
Trend Micro Endpoint Encryption	✓	✓	✓		✓	✓	✓		
WinMagic SecureDoc	✓	✓	✓		✓		✓		
See Table 1 for definitions of information protection methods.									

Source: Gartner (October 2016)

## Market Recommendations

Information theft pays big benefits to thieves, and plagues businesses with long-term damage. It is the hack that keeps on giving, since the extent of breaches is not always known, and business information can have long-term exploit value, extending into years and lifetimes in the case of some medical and financial knowledge. Once thieves have obtained your business information, they can unplug from your systems and they will be difficult to trace.

Of course, information mishandling through unplanned exposure, careless accidents and sharing are just as troubling, and trigger increasingly costly fines for compliance violations.

Security and risk management leaders who grapple with endpoint security challenges must accept that astute information protection requires a blending of several methods. Table 2 showed the capabilities of information-centric protections of listed vendors. Security planners can use this to track the breadth of information protection solutions and choose the vendors that best fit their needs.

Disk encryption remains the oldest and best defense against extraction from a lost, stolen or mishandled endpoint device. EDRM promises to be the most flexible and pervasive future technique to protect files regardless of where they travel. In between these extremes, choices should be made that match current information security concerns. For example, USB flash drives have taken on a role similar to paper, and are often handled carelessly. If a company cannot ban flash drives, then encryption controls should be added. If email and calendar on BYO devices are manifest demands that could alleviate or postpone larger access commitments, then a secure PIM can give security and risk management leaders some much-needed lead time to explore other options. Review the defense value summaries in Table 1 and choose accordingly.

Endpoint devices will continue to be an attractive hacker focus for harvesting business data. These devices are real, tangible, accessible and abundant. The users of these devices will also continue to make human errors that cause information to be vulnerable.

## Evidence

<sup>1</sup> The sluggish global economy has certainly not translated into a corresponding slowdown in criminal efforts to compromise personal information. The total number of reported data breaches reached an all-time high of 3,930 in 2015, exposing over 736 million records. "Data Breach QuickView – 2015 Data Breach Trends," (<https://www.riskbasedsecurity.com/2015-data-breach-quickview/>) Risk Based Security.



([https://www.gartner.com/technology/contact/become-a-client.jsp?cm\\_sp=bac\\_-\\_reprint\\_-\\_banner](https://www.gartner.com/technology/contact/become-a-client.jsp?cm_sp=bac_-_reprint_-_banner))

© 2016 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. If you are authorized to access this publication, your use of it is subject to the Usage Guidelines for Gartner Services ([/technology/about/policies/usage\\_guidelines.jsp](/technology/about/policies/usage_guidelines.jsp)) posted on gartner.com. The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Gartner provides information technology research and advisory services to a wide range of technology consumers, manufacturers and sellers, and may have client relationships with, and derive revenues from, companies discussed herein. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity. ([/technology/about/ombudsman/omb\\_guide2.jsp](/technology/about/ombudsman/omb_guide2.jsp))"

About (<http://www.gartner.com/technology/about.jsp>)

Careers (<http://www.gartner.com/technology/careers/>)

Newsroom (<http://www.gartner.com/newsroom/>)

Policies ([http://www.gartner.com/technology/about/policies/guidelines\\_ov.jsp](http://www.gartner.com/technology/about/policies/guidelines_ov.jsp))

Privacy (<https://www.gartner.com/privacy>)

Site Index (<http://www.gartner.com/technology/site-index.jsp>)

IT Glossary (<http://www.gartner.com/it-glossary/>)

Contact Gartner ([http://www.gartner.com/technology/contact/contact\\_gartner.jsp](http://www.gartner.com/technology/contact/contact_gartner.jsp))















Jan,

See attached.

We recently purchased Sophos encryption software and I'm looking to add it to standards. The interface is easy to use and it was fairly inexpensive.

I've sat through a number of cybersecurity seminars the past few years and they all point to encrypting laptops as a key means of protection. I sent a few feeler emails out to the region to see what everyone else was doing for this, and I don't think many are doing encryption at all yet. As I've learned, if you have a device encrypted and it's stolen, you are still covered for HIPAA related regulations. If the device is not encrypted and it's stolen, if someone suggests that you might have PII on that device (IE: a student's IEP) the onus is on the district to prove that the PII was no there, not on the person accusing the district. If the device is encrypted, you do not have to prove much else (or so I have been told).

We tried BitLocker. We ran into issues getting the key management server set correctly and management of it looked to be overwhelming. This tool uses the BitLocker software itself, but this overlays on top of it for management. The key management is then handled in the cloud by IT staff, so even if a person leaves the district or the laptop gets imaged/motherboard gets swapped, it's not a problem with encryption. There was a small cost involved, but it saved us in management time and concerns, making it a worthwhile purchase.

Thanks,

**Brian T. Richards** Manager of Network and Information Systems, Medina Central Schools.

# Sophos SafeGuard Enterprise

## Proactive Data Protection with Synchronized Encryption

Sophos SafeGuard encrypts content as soon as it is created. The encryption is always on, allowing for seamless and secure collaboration. Synchronized Encryption proactively protects your data by continuously validating the user, application, and security integrity of a device before allowing access to encrypted data. This method of always-on protection goes everywhere your data goes, making it the most comprehensive data security solution on the market.

### Highlights

- ▶ Application-aware encryption that's always on
- ▶ Synchronized Encryption proactively protects data against threats
- ▶ Comprehensive encryption across platforms and devices
- ▶ Transparent encryption process for secure collaboration
- ▶ Proof-of-compliance reporting
- ▶ Centralized key management
- ▶ Manages device encryption including BitLocker and FileVault 2
- ▶ Supports Windows, Mac, iOS, Android, and cloud-based file sharing
- ▶ Synchronizes encryption keys with Sophos Mobile Control

### Always-on encryption protects data everywhere

Sophos SafeGuard Enterprise is data-centric, automatically securing content upon creation. Once encrypted, files remain secured when shared across platforms and devices, or if they are emailed or uploaded to cloud-based file sharing programs such as Box, Dropbox, or OneDrive. This method promotes secure collaboration everywhere, working across device and platforms without compromising security and preventing accidental data leakage.

### Transparent encryption ensures user productivity

Encrypting, decrypting, and accessing information is automatic and transparent to the end user. Your users can open an encrypted file, edit it, or share it internally as they normally would. For externally sharing, decryption or creating password protected files takes only one click.

### Proactively protects data against data theft

SafeGuard Encryption has the ability to intelligently protect your data against theft. It automatically encrypts your content, and the content stays encrypted even when it's shared or uploaded to a cloud-based, file-sharing system.

Synchronized Encryption continuously validates the user, application, and device integrity. If your data ever ends up in the wrong hands, SafeGuard renders the information unusable; the files remain encrypted and unreadable.

### Real-time threat protection

SafeGuard Enterprise offers Synchronized Encryption by connecting to Sophos Endpoint Protection. The SafeGuard local agent listens to an endpoint's Security Heartbeat™ and enables automated, proactive protection. For example, in the event of an active infection, the SafeGuard agent can temporarily revoke the encryption keys, proactively protecting your data against threats. As soon as the security health of the device is restored, the SafeGuard Management Center pushes the encryption keys back to that device, restoring access to encrypted data.

## Secure external sharing with password-protected files

With SafeGuard it's simple to share content with people outside of your organization. Users can create a password-protected file with a single click of a mouse. The file is securely wrapped in an HTML 5 format, so it doesn't require the recipient to install any software. All they need is a web browser and the password to access the encrypted content.

## Mindful, one-click decryption

Users can also decrypt files to make them publicly available with one simple click. And because decryption is a logged event, you can record each instance and alert your administrator when someone attempts to decrypt a large number of files. While decryption is simple, it remains a conscious action. This inverted logic helps prevent accidental data leakage and helps to educate end users.

## Lost devices, protected data

Full-disk encryption is an essential first line of defense to protect your data in the event of a lost or stolen device. SafeGuard gives you the ability to managed Windows BitLocker and OS X FileVault 2 encryption from the SafeGuard Management Center.

## Synchronized for secure content collaboration on mobile devices

Sophos SafeGuard synchronizes your encryption keys with Sophos Mobile Control\*, giving you seamless and secure access to encrypted files on iOS and Android devices. Using Sophos Mobile Control's Secure Workspace app on a trusted device, users can view, access, and share encrypted data securely.

## Secure key recovery on Mobile Devices

Key synchronization between SafeGuard and Sophos Mobile Control\* lets users retrieve their FileVault or BitLocker full-disk encryption recovery keys directly in the Sophos Secure Workspace app on their mobile device. This helps users get back to work faster without having to contact the help desk, saving both time and IT resources.

## SafeGuard Management Center

Manage your encryption policies and keys for all of your devices using this centralized console. From the SafeGuard Management Center, you can set data security policy for groups and devices, secure, store, exchange, and recover keys. You can also generate compliance and audit reports, all from within the console.

## SafeGuard Licenses

Modules	SafeGuard Disk Encryption	SafeGuard File Encryption	SafeGuard Enterprise
Full Disk Encryption	✓	-	✓
Centrally Manage BitLocker and FileVault 2	✓	-	✓
File/Folder Encryption	-	✓	✓
Encryption for File Shares	-	✓	✓
Encryption for Cloud	-	✓	✓
Removable Media Encryption	-	✓	✓
Synchronized Encryption	-	✓	✓
Management Console	✓	✓	✓

\* Requires Sophos Mobile Control Advanced

United Kingdom and Worldwide Sales  
Tel: +44 (0)8447 671131  
Email: sales@sophos.com

North American Sales  
Toll Free: 1-866-866-2802  
Email: nasales@sophos.com

Australia and New Zealand Sales  
Tel: +61 2 9409 9100  
Email: sales@sophos.com.au

Asia Sales  
Tel: +65 62244168  
Email: salesasia@sophos.com

Oxford, UK  
© Copyright 2016. Sophos Ltd. All rights reserved.  
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK  
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

16-06-29 DSNA (DD-2378)

## Try it now for free

Register for a free 30-day evaluation  
at [sophos.com/data](https://sophos.com/data).

# SOPHOS